CHAPTER

14

DISASTER RECOVERY MECHANISMS

After reading this chapter and completing the exercises, you will be able to:

- Understand the differences between an Active Directory domain and a Windows NT domain
- Describe what happens during the Windows 2000 boot process
- Explain how the tools in the Advanced Options menu work to repair a damaged operating system
- Explain how the Emergency Repair Disk and the Recovery Console can recover Windows 2000 settings or fix a problem
- Describe how the restoration process works to restore a server to its original condition

Chapter 13 discussed the fault tolerance mechanisms available in Windows 2000 Server (and the clustering available in Windows 2000 Advanced Server and Datacenter Server). As noted in that chapter, being fault-tolerant isn't always enough. Your entire cluster could be destroyed by a fire or flood. The disk controller on your mirror set could fail, leaving you with inaccessible disks. For example, George thinks he knows how to back up the server; unfortunately, he finds out—too late—that he didn't know the procedure as well as he imagined. In fact, the server hasn't been backed up in weeks. Although this case is a hypothetical example, it's really not far from reality. Things like this happen every day.

Not all of the tools that Windows 2000 offers to help you recover from disaster work in quite the same way. Each has a different function. Some tools reverse a single action that's causing a problem; others allow you to scrap all changes and start over. Which disaster recovery tool you use to get things back up and running again depends on both your understanding of what the problem is and the tools themselves. It's critical that you pick the right tool for the job. There's nothing magical about recovery tools, after all. They restore damaged or missing files. The tool you pick to fix a damaged system depends on which files you need to replace.

What's Happening During the Boot Process?

First, let's look at what happens behind the scenes when you boot a Windows 2000 computer. As you'll see, the boot process is simply the systematic loading of the base operating system, the files needed to support the devices attached to the computer, and the services running on the computer.

Loading Basic Hardware Support

Before considering the problem of whether Windows 2000 is even working, you need to get the hardware working. In the initial stages of the boot process, the computer reads the BIOS to discover the basic hardware configuration. It then reads the disk signature on the boot disk to find the location of the bootable partition (where the operating system is stored).

As a consequence, you will not be able to boot the server if the boot drive isn't working. Thus, the drive itself, the disk controller for the boot drive, and the cable connecting the two must be operational. Additionally, the CPU and the motherboard must be up and running, as must the system BIOS. The CPU handles all processing in the computer; the motherboard is the common interface for all hardware that allows the various parts of the computer to communicate; and the BIOS describes the computer to itself.

If any of these parts is not working, skip to the section on rebuilding the server from the backups. Other hardware can give you problems, but you need all of these pieces to get the server to respond.

If you are having low-level hardware problems, restart and observe the computer to see the point at which the problem appears. Here are some points at which problems may appear and some possible solutions:

- If the computer does not boot and makes no noise when you flip (or press) the On switch, the problem is power. Check the power cord to ensure that it is working and plugged into a live power outlet. If the power source isn't the problem, the power supply in the computer might be at fault.
- If the computer comes on for half a second and then switches off just as fast, the problem probably lies in the connection of the motherboard to the power supply. The motherboard must be plugged in properly with two connections; reverse the connections, and the motherboard will short out. Older computers would let you turn on the computer and kill the motherboard, but newer ones will just cut the power if they recognize that the power supply connections are reversed.
- If the fan starts but the computer doesn't do anything else, the motherboard is probably not working and needs to be replaced.

If you don't hear the fan when you start up the computer, double-check that the fan is working even if the rest of the computer boots normally. Electronic components are very delicate and can easily overheat. The fan circulates air within the computer to keep things cool. Even if the room is comfortable, the inside of the computer (typically 15–20 degrees warmer than the ambient temperature) may be too warm.

- If you can hear the computer boot but you can't see anything (remember that you need working video to use Windows 2000) and hear a beep, the problem probably lies with the video card. Verify that it's seated properly. If its seating is not the problem, you may need to replace the video card.
- If the computer boots and can find the CD-ROM drive and floppy drive but does not find the hard disk controller, the controller has failed and needs to be replaced.
- If the computer boots and finds the hard disk controller but no bootable hard disk, the hard disk may be damaged (possibly from a virus) or not working and may need to be replaced.

Loading Ntldr

Assuming that the computer parts are all working and the computer has found the bootable hard disk, the next step is to load the operating system. The first part of Windows 2000 that loads is **Ntldr**, a small program in the root directory of the boot partition of the server's hard disk. Ntldr announces itself by displaying the boot menu for your computer. It is also doing the following:

1. Shifting the processor into 386 mode
2. Starting a very simple file system that allows Windows 2000 to boot from the hard disk
3. Reading the contents of Boot.ini to display a menu of other possible boot options
4. Accepting the choice of which operating system to load

If you choose to load Windows 2000 Server, Ntldr passes control to Ntdetect.com, which detects the hardware on your server.

Detecting Hardware

Ntdetect.com is in charge of figuring out what hardware is present on your server. It checks for the following:

- The PC's machine ID type
- The bus type (PCI, ISA, MCA, EISA)
- The video board type
- The keyboard and mouse type

- The ports detected on the computer (USB, serial, and parallel)
- The floppy drives present on the computer

Once Ntdetect has run without problems, it takes the results of its survey and uses them to build the HKLM\Hardware key of the Registry, shown in Figure 14-1. This key is rebuilt each time you restart your computer, so it is always up to date. If Ntdetect doesn't run, it is either missing or a hardware conflict exists in the server.

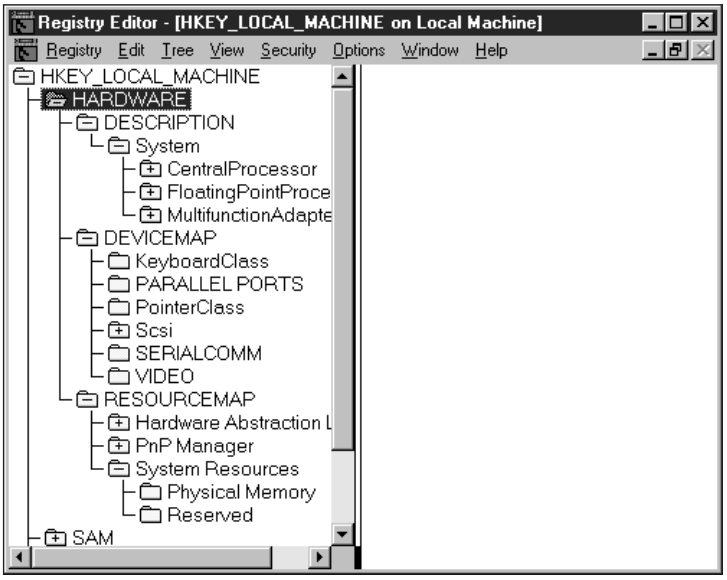

Figure 14-1 Contents of the Hardware key

Loading the Windows 2000 System Kernel

In Chapter 2, we noted that the core part of Windows 2000 is located in **Ntoskrnl.exe**, which is the "kernel" of the Windows 2000 operating system. When Ntdetect has located the hardware platform in use, it installs the hardware abstraction layer (HAL) appropriate to it and loads Ntoskrnl at the same time in four stages: loading the kernel, initializing the kernel, loading the services set to start automatically, and starting the Win32 subsystem.

Kernel Load Phase

Once Hal.dll and Ntoskrnl are loaded into memory, Windows 2000 loads the system settings into HKLM\System\CurrentControlSet\Services. It then refers to these settings to determine which drivers it must load and in what order. All services set to load during the boot phase are loaded at this time.

Are you unsure which services load when? All services currently installed on the server have keys in HKLM\System\CurrrentControlSet\Services. To find out when a service loads, open its key and look at the start value. A start value of 0 means that the service loads during the kernel load phase; a value of 1 loads the service

during the kernel initialization phase; a value of 2 loads the service automatically when the services are loading; a value of 3 indicates that the service is enabled but can be started only manually; and a value of 4 indicates that the service is disabled.

Kernel Initialization Phase

Once the kernel is loaded, it is initialized. The kernel scans for services with a start value of 1 and starts them. In addition, Windows 2000 builds a new current control set, but does not save it yet (it will not save this set until the next phase). Autochk.exe runs to verify that the file system on NTFS volumes is intact and notes the location of any bad sectors. Also, the page file is set up.

Services Load Phase

At this point, Windows 2000 loads the Services Manager and the Win32 subsystem, and starts all services with a start value of 2. Windows 2000 writes the current control set to HKLM\System.

Windows Subsystem Start Phase

The final stage of the Windows 2000 boot process involves initializing the Win32 subsystem, which supports the graphical interface for Windows 2000. Winlogon.exe, which handles interactive user logons and logoffs, starts and listens for the Ctrl+Alt+Delete sequence that means someone is trying to log on.

Advanced Options Menu

But what if the boot process doesn't work that way? Some of the most annoying problems that can plague an operating system are really simple. The **Advanced Options menu** can help you detect such flaws.

When you boot a Windows 2000 Server, you will see a short boot menu listing the operating systems installed on the computer or just Windows 2000 if it is the only operating system. If you press F8 when this menu appears, you will exit the standard boot menu and go to the Advanced Options menu, shown in the following code:

```
Windows 2000 Advanced Options Menu
Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt

Enable Boot Logging
Enable VGA Mode
Last Known Good Configuration
Directory Services Repair Restore Mode (Windows 2000 Domain
Controllers Only)
Debugging Mode

Boot Normally
Return to OS Choices Menu
```

Use the last two options to either just boot Windows 2000 Server or return to the main menu to see the available options. Starting from the top, let's look at what each of the other options can do to fix a broken Windows 2000 installation.

Safe Mode Options

Safe Mode is shorthand for "boot the operating system with the bare bones of the drivers and services it needs to run." Windows 2000 supports three kinds of Safe Mode: Ordinary Safe Mode, Safe Mode with Networking, and Safe Mode with Command Prompt.

Ordinary Safe Mode loads only the drivers and services required to boot the computer and to provide a simple operating environment. No network drivers are loaded, and network-dependent services (which normally start automatically) are set to start manually. In fact, these services are disabled—you can't turn them on from the Services tool in the Administrative Tools program group or from the Microsoft Management Console. This version of Safe Mode is useful when you need to fix problems related to network-dependent services, or when you are not sure what the problem is and don't want to take any chances, but need the GUI to resolve it.

Safe Mode with Networking is just like Safe Mode, except for the addition of network support. Choose this boot option when you want a pared-down version of the operating system, but need network support to fix something (for example, if the printer drivers you need to reload are installed on another computer, and the computer you are fixing is allowed to install printer drivers only from the trusted source).

Safe Mode (Command Prompt Only) works like Safe Mode—no networking support, basic VGA video, no extraneous drivers—except that it uses the command prompt (Cmd.exe) for a shell instead of Explorer (Explorer.exe). Use this mode if something is wrong with Explorer that keeps you from loading the graphical desktop. Although you can load any working part of the operating system from the command prompt if you know the name of the executable file that loads that component, none of the graphical pieces needs to work to start Windows 2000 in this mode. You can even receive a regular desktop if Explorer.exe works, but you're not dependent on it.

Boot Logging

Enabling **boot logging** sets up Windows 2000 to load normally, as it would if you had not interrupted the process. The only addition to the process is that Windows 2000 logs the boot process, listing all of the files loaded in support of the operating system in a file called Ntbtlog.txt. You can use this option to see which drivers did—and did not—load in the course of the boot process.

Boot logging is useful as a recovery tool only if you have previously logged the boot process at a time when everything is working properly. If you've done so, then if some component of Windows 2000 stops working, you can compare the two lists to see whether a particular file is missing. Boot logging is also turned on by default whenever you boot in Safe Mode.

Enable VGA Mode

Let us assume that you have just installed a new video card in your Windows 2000 computer. You install a new driver for it and select the video card. When testing it (Windows 2000 always has you test new resolutions to make sure that the monitor and card can support them), however, you can't see anything. You inadvertently press the Tab key and Enter, accidentally telling Windows 2000 that you want to keep these settings. Unfortunately, you can't see it well enough to restore it to a configuration that works.

Under the first version of Windows NT, you had to go through a long chain of keystrokes to fix this problem, essentially typing blind to get a vanilla video configuration. Under later versions of Windows NT and Windows 2000, however, **VGA Mode** is now a boot option.

With the VGA mode option, instead of loading the video driver that your computer is normally set to use, a plain VGA driver will be loaded that will work with any board that Windows 2000 supports. The screen may not have the high resolution to which you're accustomed, and the refresh rate (the rate at which the screen repaints itself—the higher the refresh rate, the less the screen flickers) may be uncomfortably low, but you will be able to edit the video settings so that a driver works. Fix the settings, reboot, and you have fixed the problem.

Last Known Good Configuration

Humans are fallible. So as long as they use operating systems, there should be some kind of undo feature. In Windows 2000, this feature is called the **Last Known Good Configuration**. It can't help you in every situation in which you change your system, or reboot, and then realize that the modification damaged the system. Nevertheless, it can sometimes help you reverse history by allowing you to load not the configuration that was in place when you logged off (which is normally what would happen), but the configuration that was in place the last time you successfully logged on.

The Last Known Good Configuration option in the Advanced Options menu works because of how Windows 2000 maintains configuration information. Every time you boot Windows 2000 and log on, the kernel loading phase stores the computer and operating system configuration information for the local machine in a Registry key called HKLM\System\CurrentControlSet. When Windows 2000 needs to find out its current settings, it refers to the values stored here.

To ensure that the computer can't be rendered unbootable by a single bad configuration, Windows 2000 also stores a backup copy of the configuration information. In fact, it stores a couple of copies of the computer's system settings in the Registry, as shown in Figure 14-2. (Look for CurrentControlSet001 and CurrentControlSet002.)

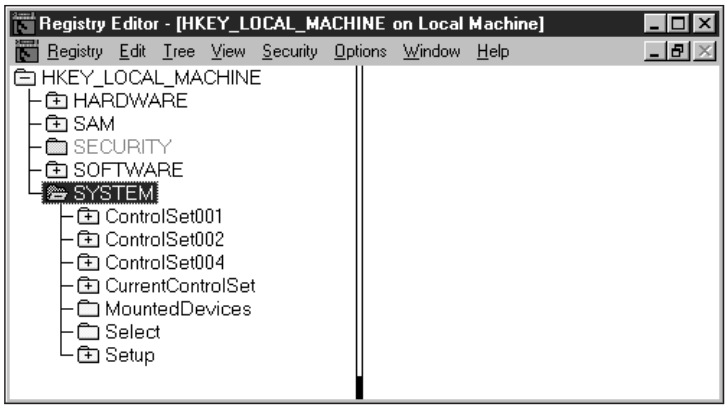

Figure 14-2 Copies of the Windows 2000 configuration settings in HKLM\System

These numbers are assigned to the configuration settings (and they're likely to be different on different machines). To find out which configuration set your Windows 2000 computer is using at the moment, look in HKLM\System\Select (see Figure 14-3).

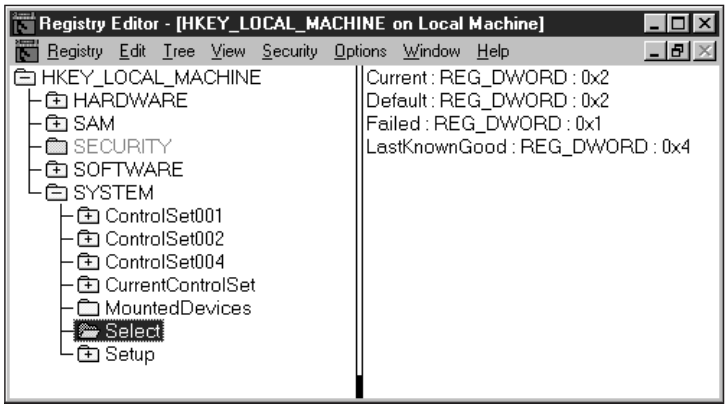

Figure 14-3 Possible values for configuration settings

Four values are shown in Figure 14-3: Current, Default, Failed, and LastKnownGood. If you restart the machine and boot normally (that is, without using the Advanced Options menu), the Default control set is used. The Failed value is the configuration set that was the default when you chose to start the machine from the Last Known Good Configuration menu. Because you instructed Windows 2000 to not start with that configuration set, it is now marked as Failed—even if nothing is actually wrong with it.

Note that this option applies only to the system configuration information, you must be able to load the Windows 2000 kernel, and its success is dependent on the settings used the

last time you booted the computer and logged on. As a result, you can't always use the Last Known Good Configuration option to reverse an error. Specifically, you cannot use the Last Known Good Configuration option in the following situations:

- You must have logged on at least once successfully. Consequently, this option won't help you if you're installing Windows 2000.
- You must use this option *before* you log on again. The settings in place when you log on are saved as the Last Known Good value and are kept for only one generation. Even if the system hangs immediately when you log on, it is too late.
- If the change you want to reverse is not part of the control set information, you can't use the Last Known Good Configuration option to reverse it. Changes to user profiles and system policies are not kept in the control set information, nor are passwords or group accounts.
- If you can't even get to the boot menu, this option is useless.

Directory Services Restore Mode

The Directory Services Restore Mode is actually the second step for restoring a domain controller. Ordinarily, you can restore the Active Directory from Windows 2000 Backup (as described in the later section, "Restoring a Server") and then log back on again normally. The Active Directory (and Certificate Server) will recheck their indices and perform an integrity check. Then, you should again be up and running.

The **Directory Services Restore Mode** is intended for those times when you want to perform a more advanced verification. When you choose this option, it will kick you back to the main boot menu, with blue text at the bottom of the screen indicating that you are in Directory Services Restore Mode. The system will boot in Safe Mode with Networking, run CHKDSK on all the volumes, and then present the logon screen for you to log on as the administrator of the local domain.

As soon as you log on, run REGEDT32 and look in HKLM\System\CurrentControlSet\Service\NTDS for a subkey called Restore in Progress, which is created by Windows 2000 Backup. The presence of this key tells the Active Directory to check all of its indices the next time it starts up in normal mode.

Once you've ensured that the Active Directory was restored properly, you can restart the computer normally. The directory should work as intended.

Debugging Mode

Debugging mode is not actually a repair mode, but rather a way of moving the system boot log to another computer for evaluation. You can use this mode to debug a boot process from a computer that won't let you get far enough in the boot process to glean any useful information from the boot log. When you select this option, Windows 2000 sends all of the boot information to the serial port, transmitting it to another computer connected to the one you are debugging with a serial cable.

Repairing a Damaged Operating System

As you can see, the Advanced Options menu is helpful mostly for problems that are not too serious. Should you run into something more drastic, you will need to use either the Emergency Repair Disk or the Recovery Console to fix the problem.

Emergency Repair Disk

The **Emergency Repair Disk (ERD)** is a simple procedure for those times when you don't know precisely what the problem is, but you want to fix the server and get it back up and running again. If you've regularly backed up your system configuration data with the ERD option in the Backup program, you should be able to restore the server to a working configuration. Essentially, when you use the ERD during a repair of this kind, you tell Windows 2000 to read the configuration files stored in a Repair\Regback directory in your Windows 2000 installation and to copy those files back to their original locations. Any files that don't match the contents of the Regback folder may be replaced.

The Repair folder contains the original Windows 2000 configuration files, so you can use the ERD to restore your operating system to its original configuration without reinstalling the operating system.

If you don't update the contents of the Repair\Regback folder regularly, it will contain old Registry information. That isn't necessarily bad, but it will restore your Windows 2000 Server to an older state. In Windows 2000, Registry information is not stored on the ERD itself—unlike the Windows NT 4 ERD.

System Recovery Console

The ERD is designed for those times when you don't know what's wrong, but you want the problem fixed right away. In contrast, the **Recovery Console** is meant for those times when you've got a pretty good idea of what the problem is and how to fix it, but something about the Windows 2000 interface or the way it works makes it impossible to do so. In many ways, the Recovery Console acts like a command-line version of Windows 2000, but with a few limitations.

For example, imagine that you have a runaway network card service, set to run automatically when you boot Windows 2000, that doesn't work properly. While it is loaded, it repeatedly releases error messages and uses up nearly 100% of the CPU time by displaying these messages. You can grab a few cycles only during the seconds between when you click OK on the error message and the instant the next error message starts up. With great difficulty and a lot of determination, you could open the Services tool in the Administrative Tools folder, find the errant tool, and disable it. Doing so would take forever, however, because you would have only a few CPU cycles in which to move the mouse, go through the various folders to find the Services tool, find the tool in the list, and then disable it.

A better option would be to disable the service without ever giving it a chance to start. You can do so from the Windows 2000 Recovery Console.

In fact, you can do all of the following from the Recovery Console:

- Copy system files from a floppy disk or CD to a hard disk
- Start and stop services
- Read and write data in the system directory on the local hard disk
- Format and repartition disks
- Write boot sectors and master boot records to disks

To get a complete list of commands available in the Recovery Console, you can type **help** at the command prompt. Table 14-1 shows the available commands.

Table 14-1 Recovery Console commands

Command Name	Function
CD or CHDIR	Displays the name of the current directory, or changes directories. Typing CD.. closes the current directory and moves you up one in the tree.
CHKDSK	Runs CheckDisk.
CLS	Clears the screen of any previous output so that you can see better.
COPY or EXTRACT	Copies files from removable media to the system folders on the hard disk. By default, it does not accept wildcards.
DEL or DELETE	Deletes one or more files. By default, this command does not accept wildcards.
DIR	Lists the contents of the current or selected directory.
DISABLE	Disables the named service or driver.
ENABLE	Enables the named service or driver.
DISKPART	Creates or deletes disk partitions.
FIXBOOT	Writes a new partition boot sector on the system partition.
FIXMBR	Writes a new master boot record (MBR) for the partition boot sector.
FORMAT	Formats the selected disk.
LISTSVC	Lists all services running on the Windows 2000 installation.
LOGON	If you have multiple Windows 2000 (or Windows NT) installations on the local hard disk, allows you to pick the installation you want to repair.
MAP	Displays the drive letter mappings currently in place. This command is handy for getting the information you need to use DISKPART.
MD or MKDIR	Creates a directory.
MORE, TYPE	Displays the contents of the chosen text file.
RD or RMDIR	Deletes a directory.
RENAME or REN	Renames a single file.
SYSTEMROOT	Makes the current directory become the system root of the drive you are logged into.
ATTRIB	Changes the attributes of a selected file or folder.
EXTRACT	Extracts a compressed installation file to the local fixed disk. It works only if you're running the Recovery Console from the installation CD.

In addition to the commands listed in Table 14-1, the Recovery Console includes a BATCH command that you can use to create jobs. When you are finished with the Recovery Console, type "exit" to restart the computer.

Unlike the other Windows 2000 recovery tools, the Recovery Console is not set up by default. You can reach it either by running Setup from the Windows 2000 CD and choosing to repair an existing Windows 2000 installation or by installing it from Windows 2000 so that the Recovery Console is included in the boot menu that appears at system startup.

Restoring a Server

You may need to rebuild your server from the ground up. To do so—and to prepare for such an eventuality—you need to understand the wedding cake of generic operating system data, system configuration data, and user data that makes up a server. Again, this restoration operation is not rocket science—it is nearly all about file replacement.

The first step to restoring a server is to reinstall the operating system from scratch. This step will replace any system executable files, DLLs, and other files that your operating system needs. If any service packs or bug fixes for Windows 2000 have been issued and you already had them installed, reinstall them after installing Windows 2000. If you don't have the same set of core operating system files available that was installed previously, you may not be able to restore the backups.

When the base operating system is available, use the Windows 2000 Backup Restore Wizard to restore the System State data from your backups. This step will restore the Active Directory certificate services (if you had them set up), the COM registration database, the system volume, the file replication service, boot files, and the Registry. When you restart the system, Active Directory should inspect its indices to verify that they're in order; it will then be ready to support the directory again. For a more hands-on approach to making sure that the system state data are ready to go, refer to the Active Directory Restore option in the Advanced Options menu.

You must watch out for the Authoritative Restore option in the Restore Wizard. If you have more than one domain controller in your domain and the Active Directory is replicated to any of these other domain controllers, you need to have that information replicated onto the other domain controllers. To ensure that the data you are restoring are replicated to these domain controllers, you must perform what's called an **authoritative restore**. Normally, the Backup Restore operation doesn't operate in authoritative mode, meaning that any data restored—including Active Directory objects—will retain the original update sequence number used by the Active Directory replication system to detect and spread Active Directory changes among the domain controllers. As a result, any data restored in nonauthoritative form look older than the other Active Directory entries and won't be replicated to the other domain controllers. In addition, the Active Directory replication system will replace the restored data with the newer data from the other domain controllers and wipe out your restore operation.

Authoritative restore solves this problem. After you've restored the system state data but before you've restarted the server, run the NTDSUTIL utility in the Windows 2000 System Tools. At the prompt, type "authoritative restore". The system state data you just restored will receive the highest update sequence number in the Active Directory replication system, so the information will be replicated throughout the domain.

If you like, you can restore user data at the same time that you restore the System State data. You don't have to restore the user data and configuration data separately, although you might want to do so if you have any doubts about restoring the System State data. Restoring in steps keeps you from wasting your time by restoring data that you can't yet use.

Chapter Summary

- You've now learned the basics of the Windows 2000 disaster recovery tools. As you can see, almost all of these tools are intended to replace files that are missing or corrupted. For this reason, it's very important that you back up your data and update the Registry backups in the Repair\Regback folder every time you make a change. You'll then be sure to have the files on hand that you need to get things back up and running.

Key Terms

Advanced Options menu — An alternative boot menu (accessible by pressing F8 when the boot menu is displayed) from which you can access the various specialized start modes available for troubleshooting purposes.

authoritative restore — A method of restoring the Active Directory information to make sure that it is the most recent copy of the information and the one that should be propagated throughout the domain.

boot logging — An advanced option that boots the computer normally but lists all files loaded during the boot process, and saving the list in a file called Ntbtlog.txt. Boot logging is enabled by default when you boot to any form of Safe Mode.

debugging mode — A mode that starts Windows 2000 normally while sending debugging information through a serial cable to another computer. It is useful when you want to examine the boot process carefully.

Directory Services Restore Mode — An advanced boot option that allows you to verify that the Active Directory has been restored from backups successfully.

Emergency Repair Disk (ERD) — A floppy disk that you can create with Windows 2000 Backup and that you can use to restore a previously saved set of configuration information (stored in %*systemroot*%\repair\regback). The ERD does not contain any configuration settings itself, just the files needed to restore the information saved on the hard disk.

Last Known Good Configuration — The configuration settings that were in place the last time you successfully booted Windows 2000. You can choose to load these settings if you boot from the Advanced Options menu and choose Last Known Good Configuration from the menu.

Ntdetect.com — A core file of Windows 2000 that inventories the computer's hardware and uses this inventory to build HKLM\Hardware. Every time you boot the machine, Ntdectect.com rechecks all hardware.

Ntldr — A core file of Windows 2000 that gets the computer ready to start running Windows 2000.

Ntoskrnl.exe — An executable image for the Windows 2000 kernel that contains the base operating system functionality.

Ordinary Safe Mode — An option that loads only the drivers and services required to boot the computer and to provide a simple operating environment.

Recovery Console — A command-line recovery interface that you can use to repair bits and pieces of Windows 2000 without replacing all configuration settings.

Safe Mode — A way of booting Windows 2000 with a minimal set of drivers. It displays the usual desktop (although using only the Vga.sys driver) and has no networking support.

Safe Mode (Command Prompt Only) — An option that works like Safe Mode—no networking support, basic VGA video, no extraneous drivers—except that it uses the command prompt (Cmd.exe) for a shell instead of Explorer (Explorer.exe).

Safe Mode with Networking — An option that is just like Safe Mode, except for the addition of network support. You would use this boot option when you want a pared-down version of the operating system, but need network support to fix something.

VGA Mode — An advanced boot option that boots Windows 2000 as usual, except that it uses the generic Vga.sys instead of the video driver you have installed. It is useful for fixing problems related to bad or incompatible video drivers.

Review Questions

1. When using the Recovery Console, you can copy system files from a floppy disk to the hard disk, but not the reverse. True or False?
2. Which of the following is not required to boot Windows 2000?
   a. A working BIOS
   b. An operational floppy controller
   c. A functioning power supply
   d. A drive controller
3. When you turn the computer on, it powers up for a second and then shuts off. You can't keep it turned on. What is most likely the problem?
   a. The motherboard is connected to the power supply incorrectly.
   b. The power supply is not functioning.
   c. The BIOS is corrupted.
   d. The drive controller is not receiving power.

4. Which tool would you use to rewrite the MBR on a disk?
   a. Emergency Repair Disk
   b. Recovery Console
   c. Last Known Good Configuration
   d. Safe Mode (Command Prompt Only)
5. Which part of Windows 2000 displays the boot menu?
   a. Ntoskrl.exe
   b. Ntdetect.com
   c. Ntldr
   d. Boot.ini
6. Which piece of Windows 2000 builds HKLM\Hardware?
7. Which of the following is the start value of a service that is set up to start automatically during the kernel initialization phase?
   a. 1
   b. 2
   c. 3
   d. 4
8. What is the start value of the disabled service?
   a. 0
   b. 2
   c. 3
   d. 4
9. When does AUTOCHK run to check the integrity of NTFS file systems?
   a. During the kernel start phase
   b. During the kernel initialization phase
   c. During the services load phase
   d. After you log on
10. Mistakenly thinking that Explorer.exe was the filename of Internet Explorer, someone erases the file in an attempt to get rid of the Web browser. Which of the following Advanced Options could you use to fix the problem?
    a. Last Known Good Configuration
    b. Safe Mode
    c. Safe Mode (Command Prompt Only)
    d. Debugging Mode

11. Under what conditions does boot logging run?
12. Which of the following problems cannot be solved with the Last Known Good Configuration option? (Choose all that apply.)
    a. You've changed the Administrator password and now don't know what it is, so you want to go back to what it was before you rebooted.
    b. You inadvertently deleted a driver.
    c. You edited a group policy and want to reverse the edit.
    d. You reconfigured the printer settings.
13. You must run Directory Services Restore Mode after replacing System State data on the computer to reindex the Active Directory. True or False?
14. Why is it important to reinstall service packs before restoring System State data?
15. You must restore system state data before restoring user data. True or False?
16. What is the name of the key that the Active Directory looks for to see that it must reindex the directory?
17. Under what conditions must you use authoritative restore?
    a. When restoring data to the server while logged in with an account other than the Administrator account
    b. When restoring data to the server from an account that is not part of the Domain Administrators group
    c. When restoring the System State data
    d. When restoring the Active Directory to a computer that is not the only domain controller in the domain
18. Your Windows 2000 boot process keeps going to a certain point and then stops. You can't figure out the problem. Which of the following repair options can help you determine where loading Windows 2000 is failing?
    a. Recovery Console
    b. Last Known Good Configuration
    c. Boot logging
    d. Debugging
19. Where is repair information (in the form of updated Registry backups) for your Windows 2000 installation stored?
    a. On the Emergency Repair Disk
    b. In the \Repair folder
    c. In the \System32 folder
    d. None of the above
20. Which Advanced Options choices do *not* start the computer in some form of Safe Mode?

HANDS-ON PROJECTS

Project 14-1

To create a boot log for your computer and examine its contents:

1. Reboot the computer. When the boot menu appears, press **F8** to open the Advanced Options menu.
2. Choose **Enable Boot Logging** from the menu (use the arrow keys to move to this option and press **Enter** when it is highlighted). You'll return to the main boot menu.
3. Choose **Microsoft Windows 2000 Server** from the boot menu and press **Enter**. Windows 2000 will boot normally.
4. After you log onto Windows 2000, open the file **Ntbtlog.txt**, which is located in %*systemroot*%. You will see a list like the one in Figure 14-4.

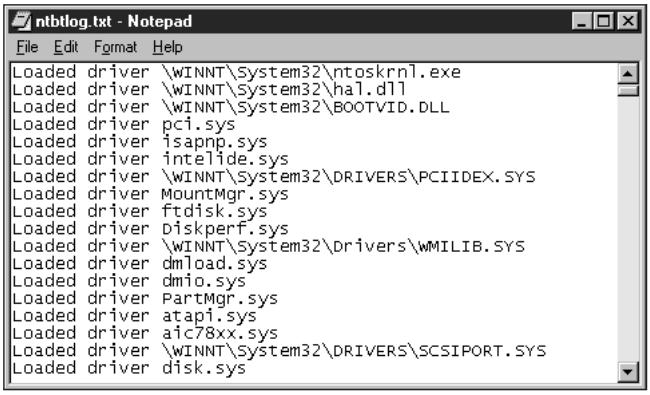

Figure 14-4 Contents of Ntbtlog.txt

Project 14-2

To change two configuration settings and see which you can restore with the Last Known Good Configuration boot option:

1. Open the **Display** applet in the **Control Panel**. Click the **Appearance** tab, and change the color scheme to something you are not currently using (in our example, we selected Rose (large)—see Figure 14-5). Apply the changes and close the applet so that you can see the new colors.

Figure 14-5 Changing the color scheme

2. From the **Date/Time Properties** applet in the Control Panel (also available if you double-click the clock on the Taskbar), change the time zone from its current setting (see Figure 14-6).

Figure 14-6 Changing the time zone

3. Restart the computer. When you reach the boot menu, press **F8** and choose **Last Known Good Configuration** from the Advanced Options menu.

4. You will be asked to choose a hardware profile (even if you haven't set one up; the default is called Profile 1). Press **Enter** or wait 30 seconds to let the default profile be chosen.
5. Windows 2000 will start normally, except that you'll see a message box indicating that Windows 2000 could not start as configured and a previous configuration was used instead. Close the message box.
6. You'll notice that the display is still a hideous shade of pink. Check the **Date/Time** properties, however, and you'll see that the time zone is back to its original setting.

The reason why one setting changed and the other did not lies in the fact that one setting was in CurrentControlSet and the other was not. CurrentControlSet does not store display colors, but it does store the date and time settings. To see which settings are reversible with the Last Known Good Configuration option, run the Registry Editor and look at the keys contained within HKLM\System\CurrentControlSet (see Figure 14-7). These keys control the services settings, the drivers loaded, the Internet settings in the hardware profiles, and other information; they do not control system colors or the existence of files, however.

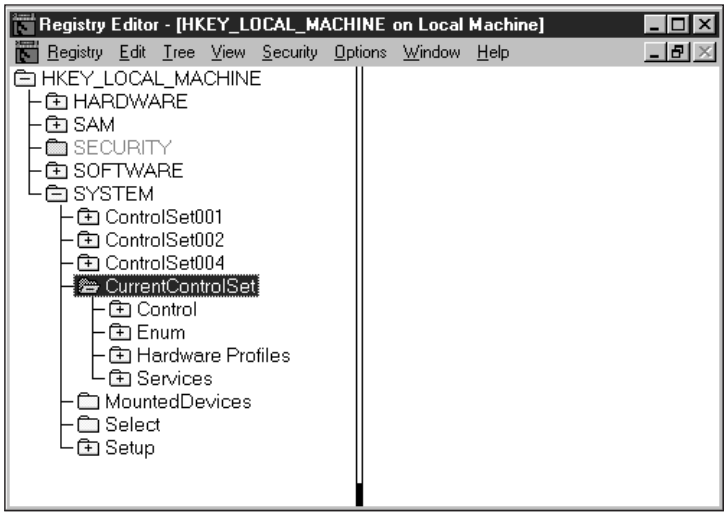

Figure 14-7 Contents of the Windows 2000 control set

Project 14-3

To install support for the Recovery Console from Windows 2000:

1. Open the **Run** tool in the Start menu, type **d:\i386\winnt32 /cmdcons** (assuming that the Windows 2000 setup files are available from drive D:), and press **Enter**. Windows 2000 will display the message box shown in Figure 14-8. Click **Yes**.

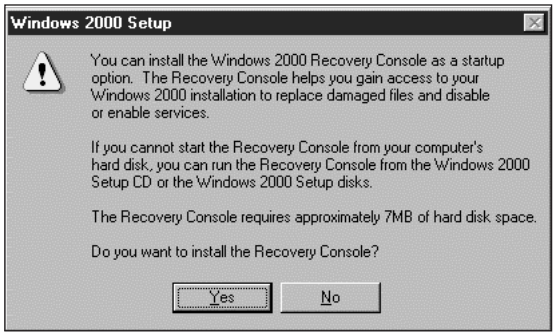

Figure 14-8 Initial screen for installing the Recovery Console (21.37)

2. Windows 2000 Setup will copy some files from the installation CD, and then prompt you to restart the computer.
3. The Recovery Console will be in the Startup menu (the text menu you see when you start up the computer) when you reboot, listed as Microsoft Windows 2000 Command Console. To start it, just choose that option before the 30-second timeout to whatever your default start-up option is.

Project 14-4

To use the Recovery Console to list services and then disable one of them, and then enable it and change its start value:

1. Reboot the system. From the boot menu, choose **Microsoft Windows 2000 Server Recovery Console**.
2. If more than one installation of Windows NT or Windows 2000 exists on the computer, choose the one you want to administer. Log into the Recovery Console using the Administrator's password.
3. In the Recovery Console, type **listsvc**. Windows 2000 will display a list of all services and drivers currently installed for that installation of Windows 2000, a short description of them, and their start type (Boot, Automatic, Manual, System, or Disabled).

Listing all of the services will probably take a few screen pages. The services are listed alphabetically, however, so you can find the one you want fairly easily. Write down its name (not case-sensitive).

4. Once you have found the suspected problem, it is time to use the disable command. The syntax is simple: **disable** ***servicename*** (choose a service and use it in place of *servicename*). Windows 2000 will then notify you that it found the Registry entry for this service (or tell you that it can't find an entry for this service, in which case you need to check your spelling and try again). It will also display the current start type and the new start type for the service. Write down the current start type for the service in case you want to start it again.
5. To make the change take effect, type **exit** to leave the Recovery Console and restart the computer.

Project 14-5

To reenable the service and then change its start type:

1. Restart the Recovery Console as described in Project 14-4. After you have logged in, refer to your notes and restart the service you disabled earlier by typing the following command: **enable *servicename*.**
2. To change the service's start type, you'll use the enable command again, but with an additional argument: **start_type**. For example, use **enable *servicename* start_type**. (If you apply this command to a disabled service, using this syntax will both enable the service and apply a start type to it.) Table 14-2 shows the available start types.

Table 14-2 Service start types available

Start Type	Meaning
Service_boot_start	Boot
Service_system_start	System
Service_demand_start	Manual
Service_auto_start	Automatic

CASE PROJECTS

1. You power up the server for the first time after rebuilding it. You can hear the drive spin up and the fan goes on, but the computer beeps at you and you cannot see any output on the screen. Which Windows 2000 disaster recovery tool should you apply to fix the problem? What do you think the problem is? Explain why the Last Known Good Configuration option can't help you if you deleted a driver that you need.
2. You attempt to start Windows 2000 one morning and see the following error message: "Windows 2000 could not start because the following file is missing or corrupt: \windows2000 root\system32\ntoskrnl.exe. Please reinstall a copy of the above file." Pressing Enter has no effect, and you see the same error message when you reboot the system. You've formatted the system partition with NTFS, so you can't get to it with a bootable floppy. What is the job of the missing file, and how can you use the Windows 2000 recovery tools to replace it?
3. Thinking that it's the executable for Internet Explorer, someone has gone to a lot of trouble to delete Explorer.exe from your Windows 2000 computer, booting to an alternative operating system so that he or she can delete the file. Now Windows 2000 won't run. What is the role of Explorer in Windows 2000, and what tool in the Advanced Options menu can you use to replace it?
4. You've restored the main domain controller (there are three) in your Active Directory structure. You notice that the information published in the Active Directory is now old—not the information that you restored to the main domain controller. What's happened, and how can you resolve this problem?